IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

SHELLY A. LEONARD, Individually and On Behalf of All Others Similarly Situated, Plaintiff, -against- US FERTILITY, LLC, Defendant.	Case No. 21-cv-835 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, SHELLY A. LEONARD, individually and on behalf of all others similarly situated, makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Plaintiff brings this action against US FERTILITY, LLC ("USF"), to obtain damages, restitution, and injunctive relief for the Class, as defined below:

> **All persons residing in New York whose personally identifiable information ("PII") was accessed during the Data Breach that affected USF's network that took place between August 2020 and September 2020.**

2. USF is one of the nation's largest providers of administrative, clinical, and information technology ("IT") services to fertility clinics, including SHER Institute for Reproductive Medicine-New York ("SHER").

3. Plaintiff sought and received treatment at SHER, which contracts with USF for IT platforms and services.

4. Plaintiff brings this class action against USF on behalf of herself and all other persons harmed by the September 2020 ransomware attack and data breach that affected patients of SHER (the "Data Breach").

PARTIES

5. Plaintiff is a resident and citizen of Huntington, Suffolk County, New York.

6. USF is incorporated in the State of Delaware and maintains its principal place of business in Rockville, Maryland.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant; there are more than 100 members of the Class; and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

8. This Court has personal jurisdiction over this action because Defendant has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

9. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL STATEMENT

A. USF's Business

10. USF holds itself out as the largest physician-owned and physician-led management services organization supporting fertility programs across the United States and internationally.

11. USF was formed in 2020 through a partnership between Amulet Capital Partners, LP ("Amulet"), a middle-market private equity investment firm based in Greenwich, CT focused exclusively on the healthcare sector, and Shady Grove Fertility ("SGF"), the largest independent fertility practice in the U.S.

12. The USF Website represents that it offers a variety of technical platforms to effectively manage clinical and business information systems, facilities and operations, finance and accounting, physician recruitment and credentialing, legal compliance, risk management, laboratory operations, business development, and fertility treatment financing programs, to name a few.

13. Collectively, the USF network currently comprises 55 locations across 10 states, including New York. Through its clinics and over 80 physicians, USF has allegedly completed nearly 25,000 in-vitro fertilization ("IVF") cycles in 2018. More than 130,000 babies have been born through the assistance of USF's partner practices.

14. Infertility is particularly sensitive and private experience. Those going through infertility treatments have reasonable expectations that their personally identifiable information ("PII") will be protected and remain confidential. Accordingly, the Data Breach is particularly egregious to the Plaintiff and other victims identified herein.

B. The Ransomware Attack and Data Breach

15. USF's website claims that it provides "Secure Data Management" with a "secure suite" of professional management services for fertility clinics.

16. In the ordinary course of doing business with USF clients such as SHER, Plaintiff and other patients are regularly required to provide sensitive, personal, and private information that is then stored, maintained, and secured by USF. This information includes or may include:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security numbers ("SSNs");
- Credit card account numbers;
- Bank account numbers;
- Educational history;
- Healthcare information;
- Insurance information and coverage;
- Photo identification;
- Employer information;
- Donor contribution information; and
- Other information that may be deemed necessary to provide care.

17. USF'S Privacy Statement provides as follows:

> As a Business Associate of the Network Practices, which are Covered Entities under the Health Insurance Portability and Accountability Act and its implementing regulations, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act (collectively, "HIPAA"), US Fertility maintains protected health information in compliance with HIPAA and our contractual obligations to the Network Practices.
>
> US Fertility uses account information in a password-protected environment as a security measure to protect your data. We use administrative, physical, and technology safeguards to ensure confidentiality and integrity of data through audit controls, access controls, and data encryption. We also use industry standard SSL/TLS encryption to enhance security of electronic data transmissions.

18. According to USF'S Privacy Statement, its collection and use of personal information is subject to applicable United States privacy laws.

19. On September 14, 2020, USF experienced an IT security event that involved the inaccessibility of certain computer systems on its network as a result of a malware infection.

20. USF responded to the Incident by retaining third-party computer forensic specialists who determined that data on a number of servers and workstations connected to USF's domain had been encrypted by ransomware.

21. The forensic investigation concluded and confirmed that the unauthorized actor acquired an unquantified number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020, when the ransomware was executed.

22. From August 12,2020 through September 14, 2020, hackers gained access to a vast trove of personal identifying information from the Data Breach, including names, dates of birth, addresses, SSNs, driver's license and state ID numbers, passport numbers, medical treatment/diagnosis information, medical record information, health insurance and claims information, credit and debit card information, and financial account information (collectively, "PII").

23. Instead of immediately notifying patients of the Data Breach, USF waited over two months. It was not until around November 2020 that USF began notifying patients of the fertility clinics using its services that its systems had been compromised by a ransomware attack. Plaintiff did not receive such notice until January 8, 2021. *See* **Exhibit A.**

24. USF notified Plaintiff on January 8, 2021 that it was "determined on December 4, 2020 that the following information relating to you was included in the impacted files when they were accessed without authorization: name and SSN, Patient Number/MPI. The impacted files may have also contained your date of birth." *Id*.

25. USF had obligations created by federal law, contracts, industry standards, common law, and privacy representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

26. Plaintiff and Class Members provided their PII to New York fertility programs and USF with the reasonable expectation and mutual understanding that such entities would comply with their obligations to keep such PII confidential and secure from unauthorized access.

27. USF failed to properly secure collection, storage and transmission of PII.

28. USF failed to maintain prevailing accepted industry standards of network and application security, internal control measures, and physical security procedures to safeguard its systems. As a result, USF left itself vulnerable to a security breach and the loss or theft of PII.

29. In connection with fertility facilities and their patients, USF failed to discharge its obligations to secure patient users' PII to comply with the mandates of the Health Information Portability and Accountability Act ("HIPAA").

30. The Data Breach caused Plaintiff and Class Members' PII, including HIPAA-protected medical information, to be disclosed to unauthorized third parties.

31. USF did not have a sufficient process or policies in place to prevent such a cyberattack, which is evident by its own statements after the Data Breach:

> USF has taken the following actions to mitigate any risk of compromise to your information and to better prevent a similar event from recurring: (1) fortified the security of our firewall; (2) utilized the forensic specialists engaged to monitor network activity and remediate any suspicious activity; (3) provided notification to potentially impacted individuals as quickly as possible. We are also adapting our existing employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails.

32. The Data Breach was the result of USF's reckless and/or negligent failure to take adequate and reasonable measures to ensure its data systems were protected, failure to disclose the

material fact that it did not have adequate computer systems and security practices to safeguard PII, failure to take available steps to prevent the Data Breach, and failure to monitor and timely detect the Data Breach.

C. Data Breaches Put Consumers/Patients at an Increased Risk of Fraud and Identify Theft

33. America faces an epidemic of data breaches that has exposed millions of individuals to identity theft and financial fraud. Criminals trade in stolen SSNs, credit card numbers, and personal information.

34. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201.

35. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

36. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance." Federal Trade Commission, Warning Signs of Identity Theft, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed Feb. 12, 2021).

37. The United States Government Accountability Office ("GAO") released a report in 2007 regarding data breaches ("GOA Report") finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record." Available at: https://www.gao.gov/new.items/d07737.pdf (last accessed Feb. 12, 2021).

38. There may be a substantial time lag, measured in years, between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the GAO:

> [L]law enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

39. Reimbursing an identity theft victim for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014. Victims of Identity Theft, available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last accessed Feb. 12, 2021).

40. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

41. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports. *See* https://www.identitytheft.gov/Steps (last accessed Feb. 12, 2021).

D. USF was on Notice of Data Breach Threats and the Inadequacy of its Security

42. USF was on notice that companies in the healthcare industry are targets for cyberattacks.

43. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)." Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug. 2014), available at: https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last accessed Feb. 12, 2021).

44. USF was on notice that the federal government has been concerned about healthcare company data encryption. USF knew it kept protected health and personal information in its computer systems and yet did not take adequate measures to secure such systems.

E. USF Failed to Comply with Federal Trade Commission Requirements

45. The FTC's publication "Protecting Personal Information: A Guide for Business" established guidelines for fundamental data security principles and practices for business. Available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Feb. 12, 2021).

46. Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a

breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

48. By allowing an unknown third party to access a USF server, USF failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential personal information data of Plaintiff and other fertility patients. For the reasons stated herein, USF's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. HIPAA and Data Breach Liability In New York

49. HIPAA is federal legislation passed in 1996 which requires providers of health care to ensure the privacy of patient records and health information. HIPAA required the federal Department of Health and Human Services ("HHS") to develop regulations to implement these privacy requirements, called the Privacy Rule, which became effective on April 14, 2003.

50. SHER contracted with the cloud service provider ("CSP") USF for administrative, clinical, and business information services and provided USF with personal information concerning Plaintiff and hundreds, if not thousands, of other fertility patients.

51. HIPAA establishes important protections for protected health information ("PHI") when created, received, maintained, or transmitted by a HIPAA-covered entity or business

associate), including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals' rights with respect to their health information.

52. Covered entities and business associates must comply with the applicable provisions of HIPAA. A covered entity is a health plan, a health care clearinghouse, or a health care provider who conducts certain billing and payment related transactions electronically. A business associate is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. A business associate also is any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

53. When SHER, a covered entity, engaged the services of USF, a CSP, to create, receive, maintain, or transmit electronic PHI ("ePHI") on its behalf, USF constitutes a business associate under HIPAA.

54. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data.

55. Lacking an encryption key does not exempt a CSP from business associate status and obligations under HIPAA. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement ("BAA"). The CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of HIPAA.

56. For providers such as SHER that are covered under HIPAA, the Privacy Rule's requirements apply to all disclosures of PHI, regardless of the purpose for which the PHI was created. The type of service rendered, and the existence of a provider-patient relationship are irrelevant in determining if the requirements of the Privacy Rule apply. Once a provider meets the regulatory definition of a healthcare provider subject to HIPAA's regulations, then that provider must comply with the Privacy Rule's requirements for all uses and disclosures of protected health information.

57. On July 25, 2019, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") amending New York's data breach notification law.

58. The SHIELD Act covers any and all persons or entities that have the private information of New York residents regardless of size or whether they are actually located in New York. Virtually every health care provider and payor in New York is already required to abide by the HIPAA and HITECH regulations covering security of PHI, but they must also comply with the SHIELD Act's provisions and make appropriate revisions to their data security compliance policies and procedures. Vendors and contractors with which private information is shared must also get into compliance with the SHIELD Act's requirements.

a. The SHIELD Act broadens the definition of "private information" to include biometric information, username/email address in combination with a password or security questions and answers, account number, and credit/debit card number.

b. The SHIELD Act expands the definition of "breach of the security of the system" to include unauthorized "access" of computerized data that compromises the security, confidentiality, or integrity of private information, and it provides sample

indicators of access. Previously, a breach was defined only as unauthorized acquisition of computerized data.

c. The SHIELD Act expands the territorial application of the breach notification requirement to any person or business that owns or licenses private information of a New York resident. Previously, the law was limited to those that conduct business in New York.

d. The SHIELD Act requires companies to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information. A company should implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal. In order to achieve compliance, a business must implement a data security program that includes at least the following:

    i. reasonable administrative safeguards that may include designation of one or more employees to coordinate the security program, identification of reasonably foreseeable external and insider risks, assessment of existing safeguards, workforce cybersecurity training, selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract, and a process for implementing adjustments to the security program based on business changes or new circumstances;

    ii. reasonable technical safeguards that may include risk assessments of network, software design and information processing, transmission and storage, implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls; and, reasonable physical safeguards that may include detection, prevention and response to intrusions, and reasonable technical safeguards that may include risk assessments of network, software design and information processing, transmission and storage, implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls; and,

    iii. reasonable physical safeguards that may include detection, prevention and response to intrusions, and protections against unauthorized access to or use of private information during or after collection, transportation and

> destruction or disposal of the information, and disposal of information after a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

59. USF did not comply with the SHIELD ACT and negligently failed to implement required safeguards and quality-control mechanisms to protect the security, confidentiality, and integrity of the PII of Plaintiff and Class Members.

60. USF negligently failed to implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.

61. USF maintained and secured the PII of Plaintiff and Class Members in a reckless manner, including, *inter alia*, failing to safeguard against ransomware attacks.

62. The PII was maintained on USF's computer networks in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff and Class Members' PII was a known and acknowledged risk to USF, which failed to take steps necessary to timely and reasonably implement protocols, training, and adjustments to its security program to mitigate and/or prevent those risks.

G. Plaintiff and Class Members' Damages

63. Personal data has value. Facebook and Google harvest billions from it through advertising. Talented hackers make a handsome living from stealing and selling it. PII is often easily taken because it is less protected and regulated than payment card data. It has been estimated that, on average, the personal data of a US resident is worth somewhere in the regions of $2000-$3000 per year. *See* http://permission.io/blog/how-much-is-data-worth/ (last accessed Feb. 12, 2021).

64. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

65. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach. While the compromise of Plaintiff's personal information was known as early as September 14, 2020, she did not receive a Data Breach Notices until January 8, 2021. *See* **Exhibit A.**

66. As a direct and proximate result of USF's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

67. As a direct and proximate result of USF'S conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

68. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

69. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

70. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

71. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

72. PII is a valuable commodity for which a market exists and is being sold by hackers on the dark web.

73. One Law Journal has stated that the value of Personal Information is a valued commodity and financial asset:

> Corporate America's increasing dependence on the electronic use of personally identifiable information ("PII") necessitates a reexamination and expansion of the traditional conception of corporate assets. PII is now a commodity that companies trade and sell. As technological development increases, aspects of day-to-day business involving PII are performed electronically in a more cost effective and efficient manner. PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.

John T. Soma, J. Z. Courson & John Cadkin, *Corporate Privacy Trend: The "Value of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH 11 (2009), available at: https://scholarship.richmond.edu/jolt/vol15/iss4/2 (last accessed Feb. 12, 2021).

74. Plaintiff and Class Members have been damaged by the unauthorized disclosure of their personal information in the subject data breach and have lost the sales value of their PII as a proximate result.

75. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial, medical accounts and records for misuse and fraud.

76. Plaintiff and Class Members have an interest in ensuring that their PII still in the possession of USF is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password-protected.

77. As a result of USF's wrongful conduct, Plaintiff and Class Members are forced to live with the knowledge that their PII — which contains the most intimate details about a person's

life, may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of their right to privacy.

78. Plaintiff and Class Members are now forced for long periods of time to endure the fear of how their PII will be used.

79. As a direct and proximate result of USF's negligent actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class").

81. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons residing in New York whose personally identifiable information ("PII") was accessed during the Data Breach that affected USF's network that took place between August 2020 and September 2020.**

82. Excluded from the Class are USF's officers, directors, and employees; any entity in which USF has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of USF. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

83. Plaintiff is a member of the class she seeks to represent.

84. This action has been brought and may properly be maintained as a class action against USF pursuant to FRCP Rule 23, because there is a well-defined community of interest in the litigation and the proposed Class is easily ascertainable.

85. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately at least 1,000 persons whose data was compromised in Data Breach.

86. Commonality: Common questions of law and fact exist for the proposed class claims and predominate over questions affecting only individual class members. Common questions include:

a. Whether USF owed a duty to Plaintiffs and members of the proposed classes to take reasonable measures to safeguard their Private Information.

b. Whether USF knew or should have known that its systems were inadequate and susceptible to a data breach.

c. Whether USF's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations.

d. Whether USF's data security systems prior to and during the Data Breach were consistent with industry standards.

e. Whether USF breached its legal duties in allowing its cybersecurity systems to be compromised.

f. Whether USF owed a duty to Plaintiff and members of the proposed classes to provide timely and adequate notice of the data breach.

g. Whether USF failed to provide notice of the Data Breach in a timely manner.

h. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of USF'S misconduct.

i. Whether USF's conduct was negligent.

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of USF's negligence and misconduct.

k. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

l. Which security procedures and data-breach notification procedure USF should be required to implement as part of any injunctive relief ordered by the Court.

87. Typicality: Plaintiff's claims are typical of the claims of the proposed Class because, among other things, Plaintiff and Class Members sustained similar injuries as a result of USF's uniform wrongful conduct and their legal claims all arise from the same core Data Breach and business practices of USF.

88. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class. Her interests do not conflict with Class Members' interests and she has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the Class.

89.

90. Predominance: USF has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from USF's conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

91. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class Action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for USF. In

contrast, the conduct of this action as a Class Action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

92. USF has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

93. Plaintiff incorporates the above allegations as if fully alleged herein.

94. USF's fertility clients required Plaintiff and Class Members to submit non-public PII in order to obtain medical care, treatment, and other healthcare services. USF had a duty to its clients, Plaintiff, and Class Members to securely maintain the PII collected.

95. By accepting this data and using it for commercial gain, USF had a duty of care to use reasonable means to secure and safeguard Plaintiff's and Class Members' PII and to prevent non-authorized disclosure of the information by cyberattack.

96. USF owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, deleting, securing, and protecting their PII from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

97. USF's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach and/or ransomware attack.

98. More specifically, this duty included among other things: (a) designing, maintaining, and testing USF's security systems to ensure that Plaintiff and Class Members' PII

was adequately secured and protected; (b) implementing adequate and effective processes to detect an intrusion into their information systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding network intrusions; and (d) maintaining data security measures at least consistent with industry standards.

99. USF's duty of care to use reasonable security measures arose as a result of the special relationship that existed between USF and its clients.

100. USF was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a ransomware attack and/or data breach.

101. USF had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

102. In New York, USF'S duty to Plaintiff and Class Members also arises under the SHIELD Act, which requires USF to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information.

103. USF's duty to Plaintiff and Class Members arose not only as a result of the statutes and regulations described above, but also because USF is/was bound by industry standards to protect PII.

104. USF also had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of its inadequate security practices. It was clearly foreseeable that Plaintiff and Class Members would

be harmed by the failure to protect their PII, because hackers routinely attempt to steal such information and use it for nefarious purposes.

105. USF breached its duties and was negligent by failing to use reasonable measures to protect Plaintiff and Class Members' PII. The specific negligent acts and omissions committed by USF include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information.

b. Failing to adequately monitor the security of their networks and systems.

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards.

d. Allowing unauthorized access to Class Members' Private Information.

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

106. It was foreseeable that USF's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the Data Breach was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches in the healthcare industry.

107. As a proximate result of USF's negligent omissions and commissions as set forth above, Plaintiff and all Class Members have sustained actual and ascertainable injury, damages and pecuniary loss as set forth above.

108. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the subject Data Breach.

109. Plaintiff and Class Members are also entitled to injunctive relief requiring USF to (i) improve and strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide sixty (60) months of complimentary access to credit monitoring and identity restoration services.

SECOND CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

110. Plaintiff incorporates the above allegations as if fully alleged herein.

111. USF is an "information fiduciary" by virtue of acting as an online service provider that analyzes, collects, uses, distributes, and sells personal information.

112. USF owed a fiduciary duty requiring reasonable care, undivided loyalty, confidentiality, full disclosure, and a duty to account to Plaintiff and Class members.

113. With respect to PII, there was and is a power imbalance which placed Plaintiff and Class Members in a position where their trust might be abused by USF.

114. There was no available methodology by which Plaintiff and Class Members could reasonably ascertain whether USF had failed to provide adequate privacy, security, and confidentiality safeguards for Plaintiff's and Class Member's PII until the Data Breach occurred.

115. USF breached its fiduciary duty to Plaintiff and Class Members by creating, causing, and permitting sensitive PII of Plaintiff and Class Members to be disclosed to non-authorized third parties between August 12, 2020 and September 14, 2020.

116. USF breached its fiduciary duty to Plaintiff and Class Members by failing to exercise reasonable care in designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' personal information was adequately secured and protected.

117. USF breached its fiduciary duty to Plaintiff and Class Members by failing to exercise reasonable care in implementing adequate and effective processes to detect system security vulnerabilities in its information systems in a timely manner.

118. USF breached its fiduciary duty to Plaintiff and Class Members by failing to exercise reasonable care in timely acting upon warnings and alerts, including those generated by its own security systems, regarding network system security vulnerabilities and intrusions.

119. USF breached its fiduciary duty to Plaintiff and Class Members by failing to exercise reasonable care in the designation and training of employees to coordinate cybersecurity compliance.

120. USF breached its fiduciary duty to Plaintiff and Class Members by failing to exercise reasonable care in maintaining data security measures at least consistent with industry standards.

121. As a direct and proximate result of USF's breach of fiduciary duty, Plaintiff and Class Members have been injured as described herein and are entitled to damages in an amount to be proven at trial.

122. Plaintiff's and Class Members' injuries include: costs stemming from the use of their PII and the diminution in its value as a result of the Data Breach; costs associated with the detection and prevention of identity theft, including purchasing credit monitoring and identity theft protection services; costs related to the loss of use of and access to their funds; adverse effects on their credit; costs associated with time spent and the loss of productivity from addressing the actual and future consequences of the data breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class.

B. For equitable relief enjoining USF from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiff and Class Members.

C. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined.

D. For an award of punitive damages.

E. For an award of costs of suit and attorneys' fees, as allowable by law; and

F. Such other and further relief as this court may deem just and proper.

[this space intentionally left blank]

DEMAND FOR TRIAL BY JURY

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands trial by jury on all questions of fact raised by this Complaint.

Dated: February 16, 2021

BROWN, LLC

/s/ Jason T. Brown
Jason T. Brown
111 Town Square Place, Suite 400
Jersey City, NJ 07310
(877) 561-0000 (office)
(855) 582-5297 (fax)
jtb@jtblawgroup.com

Attorney for Plaintiff